The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE (S) ISSUED:

05/13/2011

SUBJECT:

Multiple Vulnerabilities in Adobe Flash Player Could Allow For Remote Code Execution (APSB11-12)

OVERVIEW:

Multiple vulnerabilities have been discovered in Adobe Flash Player that could allow attackers to take complete control of affected systems. Adobe Flash Player is a widely distributed multimedia and application player used to enhance the user experience when visiting web pages or reading email messages. Successful exploitation could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Failed exploit attempts will likely cause denial-of-service conditions.

One of these vulnerabilities may be exploited if a user opens a Microsoft Word or Microsoft Excel document containing an embedded, specially crafted Adobe Flash file, which may be sent as an email attachment. **Adobe is reporting that there is malware attempting to exploit this vulnerability.**

SYSTEMS AFFECTED:

· Adobe Flash Player 10.2.159.1 and earlier versions for Windows, Macintosh, Linux and Solaris operating systems.
· Adobe Flash Player 10.2.154.28 and earlier for Chrome users.
· Adobe Flash Player 10.2.157.51 and earlier for Android.

RISK:

Government:

· Large and medium government entities: **High**
· Small government entities: **High**

Businesses:

· Large and medium business entities: **High**
· Small business entities: **High**

Home users: High

DESCRIPTION:

Adobe Flash Player is prone to multiple vulnerabilities that could allow for remote code execution. Details of these vulnerabilities are as follows:

· A design flaw that could lead to information disclosure;
· An integer overflow vulnerability that could lead to code execution;

· Five vulnerabilities involving memory corruption that could lead to code execution; and
· Four bounds checking vulnerabilities that could lead to code execution.

There have been reports indicating active exploitation of one of the vulnerabilities (CVE-2011-0627) that can be exploited by opening a Microsoft Word (.doc) or Microsoft Excel (.xls) file sent as an email attachment and embedded with a specially crafted Flash (.swf) file.

Successful exploitation could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Failed exploit attempts will likely cause denial-of-service conditions.

RECOMMENDATIONS:

The following actions should be taken:
· Install the update from Adobe immediately after appropriate testing.
· Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
· Consider installing and running Adobe Reader X in Protected Mode.
· Do not open email attachments from unknown or untrusted sources.
· Consider implementing file extension whitelists for allowed e-mail attachments.

REFERENCES:

Adobe:

http://www.adobe.com/support/security/bulletins/apsb11-12.html

SecurityFocus:

http://www.securityfocus.com/bid/46202

http://www.securityfocus.com/bid/47806

http://www.securityfocus.com/bid/47807

http://www.securityfocus.com/bid/47808

http://www.securityfocus.com/bid/47809

http://www.securityfocus.com/bid/47810

http://www.securityfocus.com/bid/47811

http://www.securityfocus.com/bid/47812

http://www.securityfocus.com/bid/47813

http://www.securityfocus.com/bid/47814

http://www.securityfocus.com/bid/47815

CVE:

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0589

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0618

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0619

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0620

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0621

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0622

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0623

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0624

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0625

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0626

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0627